ABSTRACT

A protocol appropriate for smartcard purchase applications such as those that might be completed between a terminal or ATM and a users personal card is disclosed. The protocol provides a signature scheme which allows the card to authenticate the terminal without unnecessary signature verification which is an computationally intense operation for the smart card. The only signature verification required is that of the terminal identification (as signed by the certifying authority, or CA, which is essential to any such protocol). In the preferred embodiment, the protocol provides the card and terminal from fraudulent attacks from impostor devices, either a card or terminal.